(Eddie) Jae K. Kim (CA Bar No. 236805)
LYNCH CARPENTER, LLP
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Tel.: (626) 550-1250
ekim@lcllp.com

Gary F. Lynch (admitted *pro hac vice*)
Jamisen A. Etzel (admitted *pro hac vice*)
Nicholas A. Colella (admitted *pro hac vice*)
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiff and the Proposed Class

Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
Rachel Kesten (admitted *pro hac vice*)
Yuanchen Lu (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FULLSTORY, INC., META PLATFORMS, INC., TIKTOK, INC., AND BYTEDANCE INC.

Defendant.

Case No.: 3:23-cv-00059-WHO

SECOND AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jane Doe ("Plaintiff"), individually and on behalf of all others similarly situated, asserts the following against Defendants FullStory, Inc. ("FullStory"), Meta Platforms, Inc. (f/k/a Facebook, Inc.) ("Meta"), TikTok, Inc. (f/k/a Musical.ly, Inc.) and ByteDance Inc. (collectively with TikTok, Inc., "TikTok") based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. Hey Favor, Inc. ("Favor") (formerly the "Pill Club") is a combination telemedicine company and direct-to-consumer pharmacy that prescribes its patients birth control, emergency

contraception (e.g., morning-after-pills), STI test kits, acne medicine, and prescription-strength retinol. Users can also purchase directly from Favor other menstrual care and sexual wellness products, like condoms, lubrication, and pregnancy tests, and learn from medical information it provides on health and wellness topics, like periods, skin conditions, and birth control. Visitors access these services and products through Favor's website at www.heyfavor.com and/or through its mobile app (collectively, "the Favor Platform").

2. Favor represents that its "digital primary care" platform is designed to "[m]ake healthcare more accessible." Favor is now available in 49 states and Washington, D.C. and its website receives approximately 450,000 monthly visitors. Favor states that the Favor Platform has allowed "3 million patients get access to birth control" to date.

3. Favor's services are comprised of three main components: (1) its "Medical Team" consisting of doctors and nurse practitioners who review users' health history, evaluate their needs, prescribe medications, and answer medical questions; (2) its "Pharmacy Team" comprised of pharmacists and technicians who review and process medication orders; and (3) its "Patient Care Team" who assist patients and personalize their care.

4. Customers must provide Favor with personally identifiable information ("PII") (e.g., their names, email addresses, date of birth, place of residence, payment information, and health insurance information) to use its telehealth platform. Favor also collects other identifiable information from users, including their IP address, unique device information and identifiers, and cookie data, which are used to track users across the internet.

5. Favor requires users to complete an "online consultation" that prompts users to "[a]nswer . . . health questions" before they can receive medication. These questions are highly sensitive and ask users directly for medical information, including their medical history. For example, a patient visiting the Favor Platform for birth control is asked: (1) "what type of birth control are you on?"; (2) "are you pregnant?"; (3) "how long has it been since you last gave birth?"; (4) "how frequently would you like your period?"; (5) "are you taking hormones?"; (6) "do you have any history of breast cancer?"; (7) "do you have high cholesterol medicine?"; and (8) "what other medications are you on?" Users are required to answer similar, highly sensitive medical

questions about their health to obtain emergency contraception, acne medicine, and other treatment through the Favor Platform.

6. Favor also requires users from certain states, including those in Arkansas where Plaintiff resides, to complete a separate medical consultation over video chat prior to obtaining a prescription. During this consultation, a medical professional evaluates the user, prompting them to answer additional health questions, including those about the patient's medication, medical history, and family health history.

7. Favor uses the answers to these questions to create a "digital health profile" for each user, which its Medical Team evaluates to determine treatment options and prescribe medication "if medically appropriate." Favor's Pharmacy Team sends any prescribed medication directly to the consumer, while its Patient Care Team continues to provide care after the medication is delivered by, among other things, answering questions the user may have about their medication or side effects.

8. Plaintiff and Class members provided their information to Favor based on the company's repeated assurances that their intimate health data, PII, and other information would remain protected and confidential.

9. For instance, Favor represents that it "understand[s] that medical information about [users] and [their] health is personal" and that Favor is "committed to protecting it."

10. Favor further states that it "takes the privacy of [users'] data and information very seriously" and that "***[a]ll*** of the information [Favor] hold[s] is ***treated as Protected Health Information (PHI).***" Accordingly, users' "data is held to ***even stricter privacy standard*** than required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA"), California Confidentiality of Medical Information Act, and Texas Medical Privacy Act, as some examples.)"

11. Favor goes on to ensure users that it is "required by law to make sure that medical information which identifies [users] is kept private (with certain exceptions)." These "exceptions" include the disclosure of users' information to provide medical treatment (e.g., to doctors or nurses involved in the users' treatment) and for payment processing (e.g., sending information about the

users' prescriptions to the users' health plan in order to get paid) and does not include the disclosure of users' information for marketing, advertising, tracking, or analytics.

12. Favor also promises users that it does not disclose any "personal information" to third parties, including analytics companies, and expressly represents the only information it discloses is "aggregated" and "non-identifying" and that the third parties who receive it cannot use that information "for their commercial purposes." It even states in all bold and capital letters "WE DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME."

13. Unbeknownst to Plaintiff and Class members, FullStory's, Meta's, and TikTok's (collectively "Defendants") technology was intentionally incorporated on Favor's Platform, through which Defendants intercepted users' health data and other highly sensitive information. Defendants intercepted at least users' prescription information (e.g., that they were prescribed birth control), answers to health questions (e.g., "what is your most recent blood pressure reading?" and "have you had or do you currently have breast cancer?"), medication side effects, allergies, age, and weight. In some instances, as is the case with FullStory, it intercepted ***all of the users' interactions*** on the Favor Platform (e.g., all individual clicks, keystrokes, and mouse movements), including their answers to highly sensitive medical questions.

14. This information was not aggregated or deidentified, nor were Defendants prohibited from using this information for their own benefit.

15. Plaintiff Jane Doe provided her information, including health data and PII in connection with obtaining prescriptions for birth control and emergency contraceptives, to Favor with the expectation that this information would remain confidential and private.

16. Defendants' interception of this information without consent constitutes an extreme invasion of Plaintiff's and Class members' privacy. Given the secret and undisclosed nature of Defendants' conduct, additional evidence supporting Plaintiff's claims, including the full extent of medical information Defendants intercepted, and how they used that information, will be revealed in discovery.

PARTIES

A. Plaintiff

17. **Plaintiff Jane Doe** is a resident of Hempstead County, Arkansas.

18. Plaintiff used the Favor Platform in or around the summer of 2021 to obtain medical services and products, including prescriptions for birth control, emergency contraception and condoms through the Favor Platform.

19. During the time Plaintiff used the Favor Platform, she maintained social media accounts with TikTok, Facebook, and Instagram. Plaintiff Jane Doe used the same device she used to access the Favor Platform to access these social media platforms.

20. To obtain her birth control prescriptions, Plaintiff Jane Doe was required to: (1) create a Favor account, (2) provide her PII, including her name, address, email, and health insurance information, and (3) provide her medical history and answer questions in response to Favor's health questionnaire, as described in paragraph 4-6, 13 above.

21. Plaintiff Jane Doe was also required to complete an additional medical consultation over video chat each time she wished to obtain a prescription. During this consultation, a medical professional evaluated Plaintiff Jane Doe over video and asked questions about her medical history, including what medications she takes and her family health history.

22. Plaintiff Jane Doe was required to answer additional health questions to obtain emergency contraception, including: (1) "what type of birth control do you use currently?"; (2) whether you are currently pregnant or breastfeeding; (3) what medications you take; (4) "do you have any medication allergies?"; and (5) "are you allergic to corn-containing products or food dye?".

23. Unbeknownst to Plaintiff Jane Doe, Defendants intercepted this information, including her PII, health data, prescription requests, and other activity across the Favor Platform.

24. Plaintiff Jane Doe did not consent to the interception of her data, which was never disclosed and directly contrary to the representations made by Favor.

B. Defendants

25. **Defendant Meta Platforms, Inc.** is a Delaware corporation with its principal place of business located in Menlo Park, California 94025.

26. Meta at all times knew that the incorporation of its software into the Favor Platform would result in its interception of identifiable health information and other sensitive data.

27. Meta, as the creator of its SDK and Meta Pixel, knew that it intercepted each of a user's interactions on the website or mobile application that incorporated this technology.

28. Meta has consistently come under scrutiny for incorporating its technology on websites and applications that involve the transmittal of sensitive data, including health information, yet continues to do so.

29. For instance, in February 2019, the *Wall Street Journal* published an in-depth analysis of Meta's collection of sensitive health information using its tracking technology from certain mobile applications. These reports led to a subsequent investigation by the Federal Trade Commission, who confirmed that Meta did in fact collect sensitive health information from a popular women's health app, including pregnancy data, between June 2016 to February 2019. It also confirmed that Meta went on to use this information for its own research and development. The New York State Department of Financial Services conducted a similar investigation of Meta and reached a similar conclusion, including finding that Meta did not take sufficient steps or precautions to prevent its interception of this kind of information or its use for commercial purposes.

30. Further, since at least 2016, Meta has allowed granular ad targeting based on sensitive information collected or received about individuals, including relating to at least breast feeding, ethnicities, religious beliefs, and income levels.

31. Despite this, it was not until November 9, 2021, that Meta acknowledged its use of data to target users based on "sensitive" topics, including "health" and how that was problematic. While Meta stated that it would remove this functionality in part, it later clarified that the change was limited to individuals' interactions with "content" on the Facebook platform (i.e., the "Detailed Targeting" option on Facebook) and ***did not apply to*** data intercepted through Meta Pixel or SDK or collected through other means. Thus, advertisers were still permitted to use "website custom audiences" and "lookalike" audiences to target users based on the information Meta intercepted through Meta Pixel and its SDK.

32. Further, Meta has acknowledged its interception of sensitive data, including health information, in public statements highlighting its efforts to develop a "Health Terms Integrity System" intended to filter out this type of information and prevent them from entering Meta's system.

33. However, independent investigations have confirmed these data filtration systems are not successful at preventing the interception of health data. For instance, researchers at *The Markup* found while investigating the use of the Meta Pixel on abortion-related websites that Meta's purported "filtering" system failed to discard even the most obvious forms of sexual health information, including URLs that included the phrases "post-abortion" "i-think-im-pregnant" and "abortion-pill."

34. Meta's own employees have confirmed the same, admitting that Meta lacks the ability to prevent the collection of sensitive health data or its use in ads. For example, Meta engineers on the ad and business product team wrote in a 2021 privacy overview "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"

35. Meta did not take any steps to prevent Favor from using its technology on the Favor Platform or to prevent its interception and use of Favor users' sensitive health data—like answers to health questions to obtain birth control.

36. As such, Meta's conduct was intentional despite knowing the privacy violations it caused to Plaintiff and Class members.

37. **Defendant TikTok, Inc.** is a California corporation with its principal place of business located in Culver City, California.

38. **Defendant ByteDance Inc.** is a Delaware corporation with its principal place of business located in Mountain View, California. Upon information and belief, Defendant TikTok, Inc. and ByteDance Inc. do not operate as independent corporate entities, but rather function as satellite offices of the China-headquartered company ByteDance Technology Co. Ltd.

39. Since its founding, TikTok has come under scrutiny for the types of data it collects, stores, and shares, ranging from government fines over collecting children's data to whether the app itself poses a national security risk for who it shares data with.

40. TikTok, as the creator of the TikTok Pixel, knew that it intercepted each of a user's interactions on the website or mobile application in which it is incorporated including those like the Favor Platform, which involve sensitive medical information.

41. TikTok's Pixel has come under intense scrutiny recently for its interception and collection of health data. A December 13, 2022 article by *The Markup* detailed these concerns, specifically highlighting the TikTok Pixel's presence on the Favor Platform as an example.

42. TikTok has not denied that it intercepts and collects users' sensitive medical data or that it uses that data for commercial purposes. Rather, when pressed by journalists from Consumer Reports about its concerning practice of collecting health information, TikTok responded only that it "continuously work[s] with [its] partners to avoid inadvertent transmission of such data."

43. TikTok did not take any steps to prevent Favor from using its technology on the Favor Platform or to prevent its interception and use of Favor users' sensitive data.

44. As such, TikTok's conduct was intentional despite knowing the privacy violations it caused to Plaintiff and Class members.

45. **Defendant FullStory, Inc.** is a Delaware corporation with its principal place of business at 1745 Peachtree Street NE, Suite G, Atlanta, Georgia 30309.

46. FullStory is well aware of the privacy concerns arising out of its tracking technology, including its session replay software.

47. For example, a 2017 report from researchers at Princeton University found Walgreens.com's use of session replay code was leaking website visitors' medical conditions and prescriptions to FullStory. Because users' names had been leaked earlier in website sessions, FullStory was able to link users' identities to the medicine that they were prescribed.

48. This occurred despite Walgreens using additional manual redaction tools to keep website visitors' information private. In response to the discovery, Walgreens stopped using FullStory "out of an abundance of caution." FullStory, on the other hand, took no affirmative steps to prevent its interception and identification of users through this software.

49. Other companies likewise denounced FullStory's session replay software after finding out FullStory obtained credit card information through its incorporation. For example,

clothing company Bonobos.com, announced that "We eliminated data sharing with FullStory in order to evaluate our protocols and operations with respect to their service. We are continually assessing and strengthening systems and processes in order to protect our customers' data."

50. Accordingly, FullStory understands that its software intercepts highly sensitive data, including health and medical information when used on a website or application like the Favor Platform, and that it would continue to do so as long as it remained installed.

51. FullStory did not take any steps to prevent Favor from using its technology on the Favor Platform or to prevent its interception and use of Favor users' sensitive health data—like answers to health questions to obtain birth control.

52. As such, FullStory's conduct was intentional despite knowing the privacy violations it caused to Plaintiff and Class members.

JURISDICTION AND VENUE

53. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative members of the Classes defined below, and a significant portion of putative Class members are citizens of a state different from the Defendants.

54. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a) because the amount in controversy in this case exceeds $75,000 and this action is between citizens of different states.

Meta

55. This Court has personal jurisdiction over Meta because its principal place of business is in California. Meta is also subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State, including Meta's collection of Plaintiff's sensitive health data from the Favor Platform and use of that data for commercial purposes.

TikTok

56. This Court has personal jurisdiction over TikTok Inc. because its principal place of business is in Culver City, California. In addition, this Court has personal jurisdiction over

ByteDance Inc. because its principal place of business is in Mountain View, California. Moreover, TikTok and ByteDance are subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State, including TikTok's and ByteDance's collection of Plaintiff's sensitive health data from the Favor Platform and use of that data for commercial purposes.

FullStory

57. This Court has personal jurisdiction over FullStory because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State, including relating to Favor's implementing of its session replay technology, and FullStory purposefully availed itself of the forum by, among other things, marketing and selling the session replay technology at issue in this case to Favor and other technology companies headquartered in this State.

58. FullStory's presence in California is significant and by all means intentional. Indeed, at all relevant times, FullStory targeted its provision and sale of session replay technology at California companies, including Favor, who maintain a website in California, as well as national websites that do business in California.

59. Not only does FullStory direct its business at California, but it actively sought out the benefits of the State and companies within it to assist with its collection and use of users' data. FullStory has created strategic partnerships with California-based companies to sell and implement FullStory's session replay software on its behalf in California as part of its "Partner Program."[1] For instance, FullStory utilizes CXperts, a California-based company, as an "Elite" partner to help new FullStory clients complete the FullStory onboarding process.[2] Likewise, it partners with Mentat Analytics, another California-based company, which provides consulting and optimization services to FullStory clients to create tags, events, and set up the FullStory dashboard and reports provided therein.[3] Yet another California-based company FullStory relies on to provide its services is Sigma

[1] *Bring more perfect digital experiences to your clients*, FULLSTORY, https://www.fullstory.com/partners/ (last visited February 6, 2024) (advertising its Partner Program as "the simplest way for technology and service providers to accelerate their clients' digital transformation.").

[2] *About CXperts*, FULLSTORY, https://directory.fullstory.com/cxperts (last visited February 6, 2024).

[3] *About Mentant Analytics*, FULLSTORY, https://directory.fullstory.com/mentat-analytics (last visited February 6, 2024).

Infosolutions.[4] FullStory advertises the services each of these California-based partners can provide on its website, each of which direct business to FullStory or help incorporate its products for end-clients. These partnerships are designed to, and do, further FullStory's sale and implementation of its session replay technology in California.

60. To further entrench itself in the California market, FullStory also integrates its services directly with the suite of products available in Google Cloud, a product created and operated by Google, LLC in California. FullStory is offered directly through the Google Cloud Marketplace, operated by and from Google, LLC in California, where it can be made "more broadly available."[5] FullStory's current employees, including executive officers, are based in California. FullStory's Chief Financial Officer[6], Edelita Tichepco, resides in San Francisco, California where she "oversee[s] all aspects of the company's financial operations."[7] As are other pertinent personnel like FullStory's Senior Sales Engineer[8], Senior Marketing Operations Manager[9], and Head of Revenue Operations.[10] So too are other employees, including an Enterprise Account Executive,[11] Enterprise

[4] *About Sigma Infosolutions*, FULLSTORY, https://directory.fullstory.com/sigma-infosolutions (last visited February 6, 2024).

[5] *FullStory: Empowering brands with a complete look into digital experience data*, GOOGLE CLOUD, https://cloud.google.com/customers/fullstory (last visited February 6, 2024).

[6] *Edelita Tichepco*, LINKEDIN, https://www.linkedin.com/in/edelita-tichepco-63a09515/ (last visited February 6, 2024).

[7] Edelita Tichepco, Chief Financial Officer, FULLSTORY, https://www.fullstory.com/about-us/edelita-tichepco/ ((last visited February 6, 2024).

[8] *Neha Nagesh*, LINKEDIN, https://www.linkedin.com/in/neha-nagesh/ (last visited February 6, 2024).

[9] *Caylin Canales*, LINKEDIN, https://www.linkedin.com/in/caylincanales/ (last visited February 6, 2024).

[10] *Brandie Marone*, LINKEDIN, https://www.linkedin.com/in/brandie-marone/ (last visited February 6, 2024).

[11] *Dan Flaherty*, LINKEDIN, https://www.linkedin.com/in/dan-flaherty-67a63246/ (last visited February 6, 2024).

Sales Director,[12] Onboarding Specialist,[13] Commercial Account Director,[14] Software Engineer,[15] and Advisory Information Technology Specialist.[16]

61. Former employees also were located in California, including FullStory's former Regional Vice President,[17] who boasts being the "#1 Commercial Sales Leader" at FullStory in 2021 and 2023, closing more than $6 million in deals in 2021 for the company from San Francisco, California. That the largest amount of deals in 2021 and 2023 emanated from California demonstrate that FullStory prioritized, and appealed to, the California market.

62. And FullStory seeks to hire more employees in California. For instance, FullStory advertises on "SimplyHired" for several roles, marking the relevant location as California.[18] One California-based position, the "Senior Digital Customer Success Specialist," will report directly to FullStory's Head of Digital Customer Success. It advertises the same position on LinkedIn, noting the relevant location as Los Angeles, California.[19]

63. Many of FullStory's investors and at least one board member are also located in California. For instance, GV, Kleiner Perkins and Salesforce are each based in California.[20] As is

[12] *Brian Cullen*, LINKEDIN, https://www.linkedin.com/in/brcullen/ (last visited February 6, 2024).

[13] *Sophie Schirmer*, LINKEDIN, https://www.linkedin.com/in/sophie-schirmer-017a07157/ (last visited February 6, 2024).

[14] *Audrey Folta*, LINKEDIN, https://www.linkedin.com/in/audrey-folta/ (last visited February 6, 2024).

[15] *Eran Naveh*, LINKEDIN, https://www.linkedin.com/in/erannaveh/ (last visited February 6, 2024).

[16] *John Brigden*, LINKEDIN, https://www.linkedin.com/in/johnbrigden/ (last visited February 6, 2024).

[17] *Garner White*, LINKEDIN, https://www.linkedin.com/in/garner-white-b312294/ (last visited February 6, 2024).

[18] *Senior Digital Customer Success Specialist*, SIMPLY HIRED, https://www.simplyhired.com/search?q=fullstory&l=California&job=6UK0Nz-u_WNBOOCx-B_nXzUDBFbejd0NBevgb-xpkUCmH4iHoWtDfA (last visited February 6, 2024); *Staff Security Engineer*, SIMPLY HIRED, https://www.simplyhired.com/search?q=fullstory&l=California&job=D-fGitRAEz_SiyM7iM7PIjvWAPO-bQo_WnJjugqMprpvRbsvgCEmqg (last visited February 6, 2024).

[19] *Senior Digital Customer Success Specialist*, LINKEDIN, https://www.linkedin.com/jobs/search/?currentJobId=3804583963&keywords=fullstory&origin=BLENDED_SEARCH_RESULT_NAVIGATION_JOB_CARD (last visited February 6, 2024).

[20] *About Us*, FULLSTORY, https://www.fullstory.com/about-us/ (last visited February 6, 2024).

Google, LLC, one of FullStory's investors that helped it raise $103 million in funding back in 2021.[21] So too is one of FullStory's "Board Observers" as well as board member Bruce Chizen.[22]

64. In addition to profiting from the provision and sale of its session replay technology in California to the California market, FullStory further targets the California market for session replay technology by marketing and advertising products that it knows collect highly sensitive user data directly in the state, including by hosting in-person conferences. For example, FullStory hosted a "FullStory Connect" in San Francisco, California on October 18, 2023, designed to help FullStory customers maximize the benefits of using FullStory's technology.[23] FullStory even touted speeches by its Chief Executive Officer and Vice Precedent of Product as benefits of attending.[24]

65. Likewise, FullStory attended "Opticon" in San Diego, California in November 2023, alongside its California-based partners like Google and CXperts.[25] It also attended "Google Cloud Next '23" in San Francisco, California in September 2023.[26] FullStory's physical presence in California is routine and frequent, as it is also presenting at "eTail 2024" an ecommerce and digital marketing conference hosted in Palm Springs, California at the end of February 2024.[27]

---

[21] *Maria Deutscher, Google, Dell, and Salesforce back $103M round for analytics startup FullStory*, SILICON ANGLE, (August 4, 2021), https://siliconangle.com/2021/08/04/google-dell-salesforce-back-103m-round-analytics-startup-fullstory/.

[22] *Alex Melamud*, LINKEDIN, https://www.linkedin.com/in/alex-melamud-7a9b8b1/details/experience/ (last visited February 6, 2024); *FullStory*, *FullStory Announces Record Expansion as Global Brands Turn to Digital Experience Intelligence (DXI) to Drive Growth and Transformation*, PR NEWSWIRE, (February 23, 2022), https://www.prnewswire.com/news-releases/fullstory-announces-record-expansion-as-global-brands-turn-to-digital-experience-intelligence-dxi-to-drive-growth-and-transformation-301488350.html; *Bruce Chizen*, LINKEDIN, https://www.linkedin.com/in/brucechizen/ (last visited February 6, 2024).

[23] *FullStory Connect San Francisco*, FULLSTORY, https://community.fullstory.com/events/fullstory-connect-san-francisco-31 (last visited February 6, 2024).

[24] *FullStory Connect: What you missed*, FULLSTORY, (October 25, 2023), https://www.fullstory.com/blog/connect-recap/.

[25] *FullStory*, LINKEDIN, https://www.linkedin.com/posts/fullstory_opticon-experimentation-roi-activity-7120140537881403392-_V_H?utm_source=share&utm_medium=member_desktop (last visited February 6, 2024).

[26] *FullStory,* LINKEDIN, https://www.linkedin.com/posts/fullstory_next23-genai-activity-7102651571766706176-rsmH?utm_source=share&utm_medium=member_desktop (last visited February 6, 2024).

[27] *FullStory*, LINKEDIN, https://www.linkedin.com/feed/update/urn:li:activity:7160371011400450048/ (last visited February 6, 2024).

66. FullStory itself acknowledges that it has purposefully availed itself to the laws of California. In FullStory's Data Processing Agreement that it enters into with its customers in the course of providing its session replay technology, FullStory indicates that it will comply with various data protection laws, including the California Consumer Privacy Act.[28]

67. Upon information and belief, FullStory generates substantial revenue through its California operations, advertising in California, raising of funding in California, and the provision and sale of its session replay technology to California companies, including Favor, who was based in and maintained a website in California.

68. Moreover, the entirety of FullStory's "infrastructure" is built on Google Cloud, which is operated by Google, LLC in California. FullStory's "data warehouse" which is used to "store and process huge amounts of sensitive customer data" is Google's "BigQuery" platform, likewise, operated out of California.[29] Its "frontend" and "primary source of storage" is Google's Cloud BigTable, yet another product emanating out of California.[30] FullStory uses several other Google products and services to process, house, and analyze end-user data, including Looker, Google Kubernetes Engine, and Google Cloud, all of which originate from the forum. *Id*. By availing itself of these services operated in California by a California company to build the entirety of FullStory and its ensuing data interception and processing services, FullStory has availed itself of the forum.

69. As alleged in paragraphs 134-137, FullStory purposefully directs its intentional interception of data at each of the States where end users reside. This is because the collection of data ultimately benefits FullStory, who can use the data for any purpose, and because it makes its products more attractive and beneficial because FullStory's clients who can then use the data to improve their products and services, including serving advertisements keyed off the data.

70. **Venue:** Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because a substantial portion of the conduct described in this Class Action Complaint was carried

---

[28] *Data Processing Agreement*, FULLSTORY, https://www.fullstory.com/legal/form-of-standard-dpa/ (last visited February 6, 2024).

[29] *FullStory: Empowering brands with a complete look into digital experience data*, FULLSTORY, https://cloud.google.com/customers/fullstory (last visited February 6, 2024).

[30] *Id.*

out in this District. Furthermore, Defendant Meta is headquartered in this District and subject to personal jurisdiction in this District.

71. **Divisional Assignment**: This action arises in San Mateo County, in that a substantial part of the events which give rise to the claims asserted herein occurred in San Mateo County. Pursuant to L.R. 3-2(e), all civil actions that arise in San Mateo County shall be assigned to the San Francisco or Oakland Division.

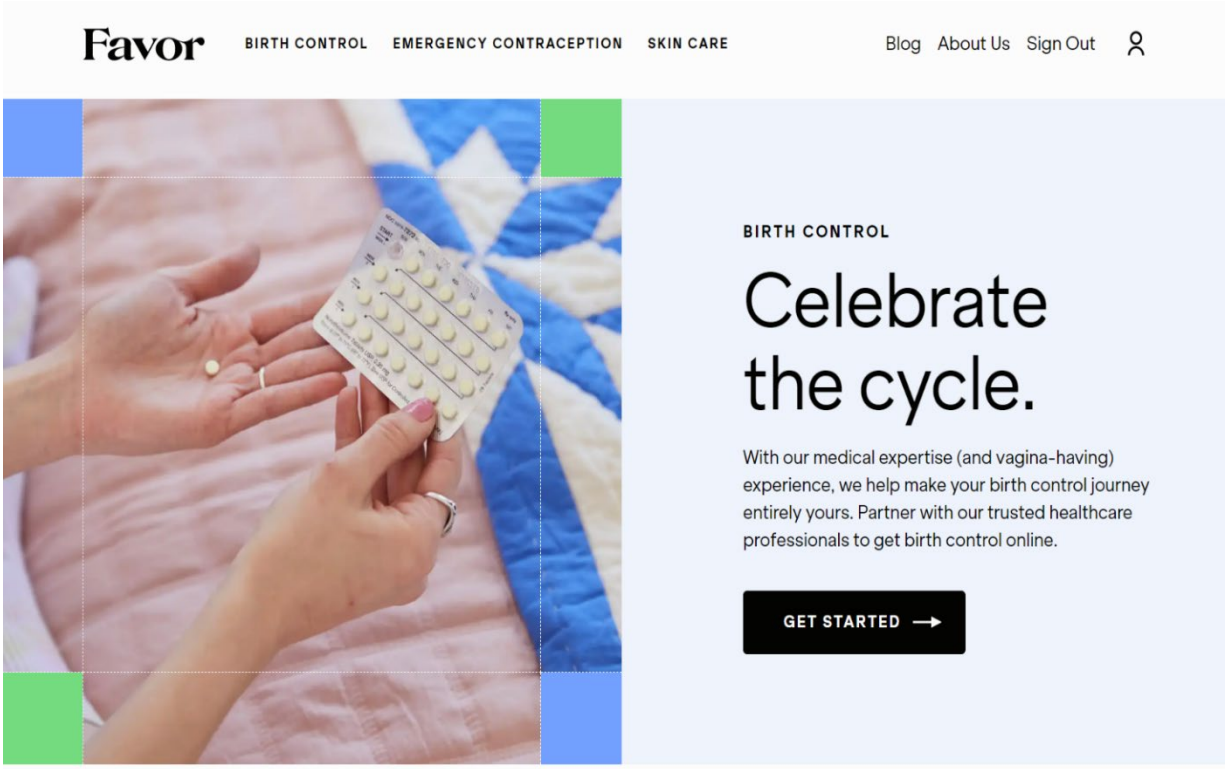
FACTUAL BACKGROUND

A. The Favor Platform

72. Favor was founded in 2016 under the name "The Pill Club."

73. The Pill Club originated as a startup telemedicine company that provided at-home delivery of birth control products. By 2021, the Pill Club had secured over $100 million dollars in financing and was servicing customers in almost all 50 States and the District of Columbia.

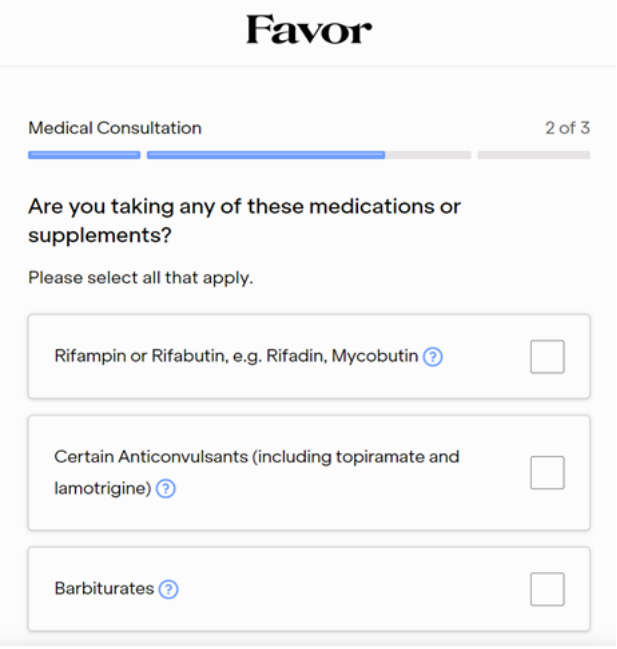
74. As the company began to expand its product offerings to skincare, menstrual products, and sexual wellness products, it rebranded itself as Hey Favor in the Spring of 2022. Now, under the more "approachable" name Hey Favor, the company has positioned itself as the go-to, "cool" provider of reproductive health medications for the Gen Z customer base.



75. Today, Favor's mission is "to create a new kind of healthcare for women and people who menstruate" through its "developed [] coalition of medical professionals, pharmacists, patient care experts, policy experts, and many more people to bring you the quality of care you deserve." Favor touts itself as providing "digital care, prescriptions and products for a better wellbeing" using "U.S. licensed medical providers," being a "licensed pharmacy" and "accepting most insurance."

76. Favor's products cover a wide range of healthcare services, from prescriptions for birth control, STI testing, to prescription skin care and over-the-counter products. Favor's most popular products are birth control (from over 120 brands), emergency contraception ("morning-after-pill"), STI (sexually transmitted infection) kits, condoms, and acne medications.

77. Before a customer can obtain a prescription for birth control from Favor, they must first create an account and answer an extensive medical history questionnaire encompassing a series of sensitive, health-related questions, in addition to providing other health-related information. The questions include: (1) "what type of birth control are you on?"; (2) "are you pregnant?"; (3) "how long has it been since you last gave birth?"; (4) "how frequently would you like your period?"; (5) "are you taking hormones?";(6) "are you breast feeding?"; (7) "are you menopausal?"; (8) "do you have history of breast cancer?"; (9) "do you have high cholesterol?"; (10) "select what other medications are you on?"; (11) "what is your blood pressure range?"; (12) "do you have heart disease?"; (13) "do you have hypertension?", and many more.



78. Likewise, a customer seeking emergency contraception must answer questions including: (1) "what type of birth control do you use currently?"; (2) whether you are currently pregnant or breastfeeding; (3) what medications you take; (4) "do you have any medication allergies?"; and (5) "are you allergic to corn-containing products or food dye?".

79. As another example, to get a prescription for acne medication, a customer must answer questions including: (1) "what are you skincare goals?"; (2) "where do you have acne?"; (3) "at what age did you start having acne?"; (4) "how would you describe your skin?"; (5) "is the skin on your face sensitive?"; (6) "do you have eczema?"; (7) "do you have rosacea?"; (8) "do you have a suspicious lesion on your face that you are concerned about?"; (9) "have you ever used any medication (prescription or over-the-counter) on your face?"; (10) "do you have any active ingredients and strengths you're interest in for treating acne?"; (11) "are you okay to experience some skin peeling and skin irritation at the beginning of your treatment?"; (12) whether you are currently pregnant or breastfeeding; (13) "do you have any allergies?"; and (14) whether you have any medical conditions, are taking any medications, or have had any surgeries.

80. Once the questionnaire is completed, the user is paired with a member of Favor's Medical Team, consisting of doctors and nurse practitioners, licensed in the users' state. The doctor or nurse practitioner "review [the users'] health history" and questionnaire results before prescribing medication based on the individual's needs if "medically appropriate." Favor also has registered nurses who are available to answer any medical-related questions a customer may have.

81. Favor's Pharmacy Team, encompassing pharmacists, intern pharmacists, and pharmacy technicians, then review and process the prescription. Favor accepts most health insurance policies and Medicaid and offers cash pricing to those that are uninsured.

82. After the prescription is received, members of Favor's Patient Care Team are available to answer any additional questions the user may have relating to the prescription, side effects, or treatment plan.

83. In addition to providing medical care and prescriptions, Favor also offers over-the-counter sexual and reproductive healthcare products and skincare. Users can purchase condoms, female condoms, pregnancy tests, and moisturizers, among other products.

84. Favor also provides medical information to individuals through its blog, which contains a variety of articles relating to sexual wellness, reproductive health, medication, and side effects to certain products. For instance, Favor features an article on its website "What Birth Control is best for PCOS?" (polycystic ovary syndrome) and another titled "Bleeding After Plan B: Causes & Side Effects."

B. Favor's Promises to Users & Sharing of Data

85. Favor pledges to users that it "takes the privacy of [users'] data and information very seriously" and that "***[a]ll*** of the information [Favor] hold[s] is ***treated as Protected Health Information (PHI).***" Accordingly, users' "data is held to ***even stricter privacy standard*** than required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA"), California Confidentiality of Medical Information Act, Texas Medical Privacy Act, as some examples.)"

86. Favor promises users that it does not disclose to third parties, including analytics companies, ***any*** "personal information." Favor claims the only information it shares is "aggregated" and "non-identifying" and that third parties cannot use information "for their commercial purposes."

87. It then states it all bold and capital letters "WE DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME."

88. Given these representations and the types of services Favor provides, users like Plaintiff and Class members expected their data, including health information, and other interactions on the Favor website, to remain confidential.

89. Despite these promises, Defendants' tracking technology was incorporated on the Favor Platform, through which Defendants intercepted highly sensitive personal and medical information Plaintiff and Class members entered on the Favor Platform, including their PII, prescriptions, answers to health questions (described above), medication side effects, allergies, age, and weight.

90. With respect to FullStory, it intercepted ***all of the users' interactions*** on the Favor Platform—i.e., every click, tap, scroll, mouse movement and keystroke—including the highly sensitive medical information users entered into the Favor Platform when seeking treatment.

C. TikTok's Tracking Technology on the Favor Platform

91. TikTok has more than 750 million monthly users worldwide and is one of the top five largest social media companies. TikTok's main source of revenue is selling ads, with reports showing that TikTok's ad revenue for this year alone surpassed $12 billion.

92. TikTok's parent company reports similar growth with its advertising revenue increasing year to year, jumping from just $7.3 billion in 2018 to $38.6 billion by 2021.

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$58 billion	$38.6 billion	66%
2020	$34.4 billion	$30 billion	87%
2019	$17.15 billion	$16.5 billion	96%
2018	$7.4 billion	$7.3 billion	98%

93. To increase its advertising revenue, TikTok offers tracking and analytics services, including the TikTok Pixel. More than a million websites, including Favor, incorporate the TikTok Pixel.

94. The TikTok Pixel is a piece of HTML code placed on a website that tracks users' interactions, including what pages they view, buttons they click on, and information they enter, along with a unique identifier.

95. The TikTok Pixel intercepts these communications immediately after they are sent and before they are received by the website operator.

96. In addition, the TikTok Pixel collects identifiable information such as the users' IP address, the device make, model, and operating system, browser information, a unique session ID, and first and third party cookie data that can be associated with a specific user.

97. TikTok uses the cookies it collects and/or its "Advanced Matching" feature to "recognize and learn about people from [the] website and the types of actions they do or don't take." In April 2022, TikTok made its collection of first- and third-party cookies automatic across all websites that incorporated the TikTok Pixel prior to March 10, 2022.

98. Once the TikTok Pixel intercepts this data, it is sent to TikTok's server, where it is stored and processed. The data collected by TikTok is then used to match website actions to

individuals, as well as provide attribution reports and track users. Further, if the user has a TikTok account, the data is used in connection with TikTok's advertising services.

99. The TikTok Pixel is incorporated on the Favor Platform. Through this technology, TikTok intercepted Favor users' interactions with the Favor Platform, including personal information. As a result, information Plaintiff Jane Doe provided to Favor to obtain birth control, emergency contraception, and condoms was intercepted by TikTok.

100. Plaintiff Jane Doe did not consent to the interception of her data by TikTok. TikTok's interception of Plaintiff Jane Doe's sensitive data without her consent is an invasion of privacy and violates several laws, including the California Confidentiality of Medical Information Act ("CMIA") and the California Invasion of Privacy Act ("CIPA").

D. Meta's Tracking Technology on the Favor Platform

101. Meta is one of the largest advertising companies in the country. To date, Meta generates nearly 98% of its revenue through advertising bringing in a grand total of $114.93 billion.

102. Meta's advertising business began back in 2007 with the creation of "Facebook Ads," which was marketed as a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."

103. Today, Meta provides advertising on its own platforms, such as Facebook and Instagram, as well as websites outside these apps through the Facebook Audience Network. Facebook alone has more than 2.9 billion active users.[31]

104. Meta's advertising business has been extremely successful due, in large part, to Meta's ability to target people at a granular level. "Among many possible target audiences, [Meta] offers advertisers," for example, "1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"

105. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Meta's advertising services. Meta generates substantially all of its revenue from selling advertisement placements:

[31] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$117.93 billion	$114.93 billion	97.46%
2020	$85.97 billion	$84.17 billion	97.90%
2019	$70.70 billion	$69.66 billion	98.52%
2018	$55.84 billion	$55.01 billion	98.51%

106. One of Meta's most powerful advertising tools is the Meta Pixel, formerly known as the Facebook Pixel, which launched in 2015 and its software development kit (SDK).

107. Meta touted the Meta Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." According to Meta, to use the Meta Pixel an advertiser need only "place a single pixel across [its] entire website to report and optimize for conversions" so that the advertiser could "measure the effectiveness of [its] advertising by understanding the action people take on [its] website." The Meta Pixel is incorporated on 6.7 million websites, including Favor's website.

108. Similar to the TikTok Pixel, the Meta Pixel is a snippet of code embedded on a third-party website that tracks a users' activity as the users navigate through a website. As soon as a user takes any action on a webpage that includes the Meta Pixel, the code embedded in the page re-directs the content of the user's communication to Meta while the exchange of the communication between the user and website provider is still occurring.

109. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. The Meta Pixel sends each of these pieces of information to Meta with other identifiable information, such as the users IP address. Meta stores this data on its own server, in some instances, for years on end.

110. This data is often associated with the individual users' Facebook account. For example, if the user is logged into their Facebook account when the user visits Favor's website, Meta receives third party cookies allowing Meta to link the data collected by the Meta Pixel to the specific Facebook user.

111. Meta can also link the data to a specific user through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users, including Facebook users.

112. Lastly, Meta can link user data to individual users through identifying information collected through the Meta Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.

113. Importantly, even if the Meta Pixel collects data about a non-Facebook user, Meta still retains and uses the data collected through the Meta Pixel in its analytics and advertising services. These non-users are referred to as having "shadow profiles" with Meta.

114. At the time Plaintiff Jane Doe used the Favor Platform, she maintained active Facebook and Instagram accounts. Plaintiff Jane Doe accessed the Favor Platform from the same device she used to visit Facebook and Instagram, and Meta associated the data it collected about her from the Favor Platform with her Facebook and Instagram accounts.

115. Meta offers an analogous mobile version of the Meta Pixel known as a software development kit (SDK) to app developers. Meta's SDK allows app developers "to track events, such as a person installing your app or completing a purchase." By tracking these events developers can measure ad performance and build audiences for ad targeting.

116. Meta's SDK collects three types of App Events. Automatically Logged Events "logs app installs, app sessions, and in-app purchases." Standard Events are "popular events that Facebook has created for the app." Custom Events are "events [the app developer] create that are specific to [the] app."

117. Once the data intercepted through the Meta Pixel or SDK is processed, Meta makes this data available through its Events Manager, along with tools and analytics to reach these individuals through future Facebook ads. For instance, this data can be used to create "custom audiences" to target the user, as well as other Facebook users who match members' of the audiences' criteria.

118. In addition to using the data intercepted through the Meta Pixel and the SDK to provide analytics services, Meta uses this data to improve its personalized content delivery,

advertising network, and machine-learning algorithms, including by improving its ability to identify and target users.

119. Meta has no way to limit or prohibit the use of data collected through the Meta Pixel and its SDK given Meta's open systems and advanced algorithms.

120. According to leaked internal Meta documents, one employee explained "You pour that ink [i.e., data] into a lake of water . . . and it flows . . . everywhere . . . How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?"

121. In these same leaked documents, another employee explained Meta does "not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, that is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation." Thus, once the data enters the Meta system, either through its SDK or Pixel, the data can be used for any and all purposes.

122. Meta's own employees confirmed no one at Meta can state confidently where all the data about a user is stored and used. In a recent court hearing as part of the Cambridge Analytica scandal of 2018, Meta's own engineers testified there was not a "single person" at Meta who could answer that question.

123. The Meta Pixel and SDK are incorporated on the Favor Platform. As a result, Meta intercepted users' interactions on the Favor Platform. For instance, Meta received users' specific responses to medical history and other health questions Favor asked in connection with a visit for birth control. This included highly sensitive medical information as reflected in paragraphs 4-6, 13, 65-68 above.

124. Plaintiff Jane Doe provided her PII, health information, and other sensitive data to Favor to obtain birth control, emergency contraception, and condoms, this information was sent to Meta.

125. Plaintiff Jane Doe did not consent to the interception of her data by Meta. Meta's interception of Plaintiff Jane Doe's PII, health data, and other highly sensitive information without her consent is an invasion of privacy and violates several laws, including the CMIA and CIPA.

E. FullStory and Session Replay

126. FullStory was founded in 2014 and is a data analytics company that offers a variety of products, from data collection to analytics. The company raised close to $170 million in funding and is valued at over $1.5 billion as of August 4, 2021.

127. FullStory is one of the leading session replay companies in the market today, touting its capabilities as "a modern way to collect user experience data" where "the amount of valuable information FullStory captures is second to none . . . ."

128. According to FullStory, "A website represents thousands and thousands of UX [user experience] decisions, and with FullStory [they] can 'watch' sessions and frequently uncover opportunities."

129. FullStory "watch[es] sessions" through sophisticated session replay code that runs in the background of any given website or mobile application. Its session replay code makes a "detailed accounting of every action that takes place on [the] site or app. From mouse movements and clicks to screen swipes or typing." Each of these pieces of data are bundled, transmitted, and then "store[d] and organize[d]" by FullStory on their platform, along with a unique identifier (i.e., UserID and SessionID) for each particular user whose communications they intercept.

130. As a result, website visitors' interactions with and communications on websites that incorporate this software, like the Favor Platform, are intercepted by FullStory in real-time.

131. In 2022 alone, FullStory intercepted and "analyzed" "1.44 trillion total events, 79 billion pages, and 25 billion sessions (including 22 billion on the web and 3 billion on native mobile apps)." Stated differently, the equivalent of "80,000 years of user activity."[32] This data is a treasure trove to companies like FullStory and those with whom they share this data.

[32] *FullStory: Empowering brands with a complete look into digital experience data*, FULLSTORY, https://cloud.google.com/customers/fullstory (last visited February 6, 2024).

132. Once this data is intercepted, FullStory provides a dashboard platform that provides its clients "access [to] data that's automatically indexed, fully retroactive, and instrumentation-free to get insight into all digital interactions." On FullStory's dashboard, its clients are able to filter the sessions and identify users based on their actions on the site.

133. Not only does FullStory intercept vast amounts of data from its clients' websites, it also leverages that data to provide analytics insights such as factors impacting the sites conversions and device-specific bugs. It also supplies custom conversion analyses using its "extensive searchable data."

134. Recognizing the value and utility of this data, FullStory reserves the right to use this data to "monitor and improve [its] Services."[33] It further states, "[f]or the avoidance of doubt" that it is granted the right to "use, reproduce and disclose" this data so long as it is purportedly "de-identified" for "product improvement" as well as any "other purposes" as it sees fit.[34] This right survives the "termination" of agreements with FullStory clients.[35]

135. FullStory's respective Data Processing Agreement with its customers states that FullStory may "share any Customer Data for cross-context behavioral advertising" so long as it obtains consent from the "Customer," i.e., the business deploying its service, ***not*** the end user.[36] It likewise states that it can "merge Customer Data with other data, or modify or commercially exploit any Customer Data" so long as the Customer agrees.[37]

136. FullStory admits the same in its Privacy Policy, stating that it will use "aggregated" or purportedly "de-identified" data in its "discretion" including for "research, analysis, modeling, marketing, and improvement of [its] Services."[38]

---

[33] *Terms & Conditions*, FULLSTORY (June 4, 2020), https://www.fullstory.com/legal/terms-and-conditions/.

[34] *Id.*

[35] *Id.*

[36] *Data Processing Agreement*, FULLSTORY, https://www.fullstory.com/legal/form-of-standard-dpa/ (last visited February 6, 2024).

[37] *Id.*

[38] *FullStory Privacy Policy*, FULLSTORY, (January 1, 2023) https://www.fullstory.com/legal/privacy-policy/.

137. Even worse, not only does FullStory retain virtually all control over how it uses the data, but it further discloses the data to one of the largest advertisers in the world, Google, LLC. FullStory discloses end-user's data to Google for its own purposes, including "processing" and "storage" through Google's "BigQuery."[39] FullStory also "sends data to Google" so that it can utilize "AI modeling and ML analytics."[40] Upon information and belief, FullStory's transmittal of data to Google were the building blocks for the companies' consequential partnership for "Advanced Generative AI" announced in 2023.[41]

138. While FullStory claims that it "requires users to block sensitive information from being recorded," it does not have the capability to do so and does not enforce that policy. As explained in paragraphs 47-49 above, researchers have shown that FullStory's "automated redaction process," which purportedly prevents sensitive information like health data from being recorded, does not successfully remove that data.

139. FullStory's session replay software is incorporated on the Favor Platform. As a result, FullStory intercepted each of its users' interactions on the Favor Platform along with a unique ID that can individually identify the user. For instance, FullStory received users' type of medication, side effects, and allergies, as well as other responses to health questions. Thus, if a user previously used a birth control with side effects, FullStory intercepted this information along with the name of the medication.

140. Plaintiff Jane Doe provided her PII, health information, and other sensitive data to Favor to obtain birth control, emergency contraception, and condoms, this information was intercepted by FullStory.

---

[39] *Data Processing Agreement*, FULLSTORY, https://www.fullstory.com/legal/form-of-standard-dpa/ (last visited February 6, 2024); *FullStory: Empowering brands with a complete look into digital experience data*, FULLSTORY, https://cloud.google.com/customers/fullstory (last visited February 6, 2024).

[40] *Id.*

[41] *FullStory Partners with Google Cloud to Develop Advanced Generative AI Features That Transform How Businesses Optimize the Digital Experience*, FULLSTORY, (June 21, 2023) https://www.businesswire.com/news/home/20230621505428/en/FullStory-Partners-with-Google-Cloud-to-Develop-Advanced-Generative-AI-Features-That-Transform-How-Businesses-Optimize-the-Digital-Experience.

141. Plaintiff Jane Doe did not consent to the interception of her data by FullStory. FullStory's interception of Plaintiff Jane Doe's PII, health data, and other highly sensitive information without her consent is an invasion of privacy and violates several laws, including the CMIA and CIPA.

F. Plaintiff and Class Members Do Not Consent to Defendants' Conduct

142. Plaintiff and Class members had no way of knowing that Defendants were intercepting their communications when interacting with the Favor Platform because their software is inconspicuously incorporated in the background.

143. This conduct is all the more egregious given the nature of the information entered into the Favor Platform, e.g., PII, requests for prescriptions, and identifiable medical information, among other things. Plaintiff and Class members would not expect this information to be intercepted without their consent.

144. This is especially true given Favor's consistent representations that this information would remain private and confidential. Favor promises that it "takes the privacy of [users'] data and information very seriously" and that "***[a]ll*** of the information [Favor] hold[s] is ***treated as Protected Health Information (PHI).***" Accordingly, users' "data is held to ***even stricter privacy standard*** than required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA"), California Confidentiality of Medical Information Act, Texas Medical Privacy Act, as some examples.)"

145. It later states that it "understand[s] that medical information about [users] and [their] health is personal" and that Favor is "committed to protecting it" and, further, that no "personal information" would be intercepted by third parties, including analytics companies.

146. Doubling down, it then states in all bold and capital letters, Favor ensures users "WE DO NOT SELL OR MARKET YOUR PERSONAL INFORMATION AT ANY TIME." It claims that it only discloses "aggregated" and "non-identifying" information and, even then, that third parties cannot use information "for their commercial purposes."

147. Favor repeats these assurances throughout its privacy policy, stating that it is "required by law to make sure that medical information which identifies [users] is kept private (with certain exceptions)." These "exceptions" include the disclosure of users' information for things like

treatment and law enforcement needs and do not include the disclosure of users' information for marketing, advertising, tracking, or analytics purposes to companies like Defendants.

148. Accordingly, Plaintiff and Class members did not consent to Defendants' conduct.

G. Plaintiff and Class Members have a Reasonable Expectation of Privacy in their User Data

149. Plaintiff and Class members have a reasonable expectation of privacy in their communications on the Favor Platform, including their health information.

150. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

151. For example, a recent study by *Consumer Reports* shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them. Moreover, according to a study by *Pew Research Center*, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

152. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.

153. Another recent study by DataGrail revealed that 67% of people were willing to pay $100 or more annually to keep their information out of the hands of companies and the government. The same study revealed that 75% of people would abandon brands that do not take care of their data.

154. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' intimate health data. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance

and how much you pay for that coverage, increase the rate you're charged on loans, and leave you vulnerable to workplace discrimination.

155. This data is also extremely valuable. According to Experian, health data is a "gold mine" for healthcare companies and clinicians.

156. Consumers' health data, including what prescriptions they have, are extremely profitable. For instance, Datarade.ai advertises access to U.S. customers names, addresses, email addresses, telephone numbers who bought brand name medicine. The starting price for access to just some of this data was $10,000. Other companies, like Pfizer, spend $12 million annually to purchase health data and the medical data industry itself was valued at over $2.6 billion back in 2014.

157. Defendants' surreptitious interception of Plaintiff's and Class members' private communications, including PII, health information, and other sensitive data violates Plaintiff's and Class members' privacy interests.

TOLLING, CONCEALMENT, AND ESTOPPEL

158. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

159. Defendants' software was secretly incorporated into the Favor Platform, providing no indication to users that they were interacting with sites that shared their data, including PII and medical information, with third parties.

160. Defendants had exclusive knowledge that the Favor Platform incorporated its software, yet failed to disclose that fact to users, or that by interacting with the Favor Platform, Plaintiff's and Class members' sensitive data, including PII and health data, would be intercepted by third parties.

161. Plaintiff was, at all times, diligent in using the Favor Platform. Nevertheless, Plaintiff and Class members could not with due diligence have discovered the full scope of Defendants' conduct, including because it is highly technical and there were no disclosures or other indication that would inform a reasonable consumer that third parties, including Defendants, were intercepting, data from the Favor Platform.

162. The earliest Plaintiff and Class members could have known about Defendants' conduct was shortly before the filing of this Complaint through the investigation of counsel.

163. Defendants were under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendants are therefore estopped from relying on any statute of limitations under the discovery rule.

164. Additionally, Defendants engaged in fraudulent conduct to prevent Plaintiff and Class members from discovering the interception of their data. Favor misled Plaintiff and Class members to believe their data, including health information and PII, would not be intercepted.

165. Favor represented to Plaintiff and Class members that they applied even stronger restrictions on the sharing of data than those imposed by HIPAA and the CMIA. It also promised Plaintiff and Class members that their "personal information" would not be shared. No Defendant disclosed the misconduct alleged herein.

166. Meta concealed in its Privacy Policy that it collects PII and medical information from Favor Platform users, as well as *any* form of medical information from *any* source. Meta maintains a Privacy Policy through which it purports to help users "understand what information we collect, and how we use and share it." Meta claims it is "important to [Meta] that [users] know how to control [their] privacy."[42]

167. This was false. Meta does not disclose, in this purportedly comprehensive policy, that it will collect medical information and PII from Favor users. Quite the opposite, Meta represents in its Privacy Policy it only collects "information when you visit [a] site or app" when its "partners . . . have the right to collect, use and share your information before giving it to us." *Id*. This, combined with Favor's own representations, would lead Favor users to believe their medical information and PII was not collected or used by Meta because Favor promised and disavowed that it would share this type of information.

168. TikTok too concealed its own data interception practices. Like Meta, TikTok maintains a Privacy Policy that states it is "committed to protecting and respecting your privacy"

[42] *Privacy Policy*, META PLATFORMS, INC. (effective December 27, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

such that it provides a policy that "explains how we collect, use, share, and otherwise process the personal information of users and other individuals age 13 and over."[43] The only sentence in this long policy that could remotely apply to the collection of Favor users' data states "Some of our advertisers and other partners enable us to collect similar information directly from their websites or apps by integrating our TikTok Advertiser Tools (such as TikTok Pixel)." TikTok could disclose, but concealed, who these "partners" were and that the vague "similar information" it referenced that it *may* collect included highly sensitive medical information and PII. TikTok did not, choosing to conceal this information to continue collecting it undetected. *Id*.

169. The same is true of FullStory. FullStory maintains a privacy policy that purports to disclose the "information [it] collect[s]." FullStory represents that it only collects "non-sensitive text" from end users and, moreover, "requests that all Customers provide notice to their website or mobile application visitors that they use the FullStory Service." FullStory concealed, and did not disclose, that one of these "Customers" was Favor and that it was, in fact, collecting highly "sensitive" information, including medical information.[44]

170. Plaintiff and Class members were not aware that Defendants intercepted their data, including PII and health information.

171. Plaintiff and Class members exercised due diligence to uncover the facts alleged herein and did not have actual or constructive knowledge of Defendants' misconduct by virtue of their fraudulent concealment.

172. Accordingly, all statute of limitations are tolled under the doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

173. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

[43] *Privacy Policy*, TIKTOK, INC., (last updated January 24, 2024), https://www.tiktok.com/legal/page/us/privacy-policy/en?enter_method=bottom_navigation.

[44] *FullStory Privacy Policy*, FULLSTORY, (effective January 1, 2023) https://www.fullstory.com/legal/privacy-policy/.

Nationwide Class: All natural persons in the United States who used the Favor Platform and whose communications and/or data were intercepted by Defendants.

174. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

175. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of millions of individuals, and the members can be identified through Favor's records.

176. **Predominant Common Questions:** The Class' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

- Whether Defendants violated Plaintiff's and Class members' privacy rights;
- Whether Defendants' acts and practices violated the Common Law Invasion of Privacy;
- Whether Defendants were unjustly enriched;
- Whether Defendants' acts and practices violated California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*;
- Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*;
- Whether Plaintiff and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and
- Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

177. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. The claims of Plaintiff and the members of the Class arise from the same conduct by Defendants and are based on the same legal theories.

178. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendants have no defenses unique to any Plaintiff. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to the interests of the other members of the Class.

179. **Substantial Benefits:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

180. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

181. California substantive laws apply to every member of the Class. California's substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiff and Class members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

182. Meta and TikTok maintain their principal places of business in California and conduct substantial business in California, such that California has an interest in regulating Meta and TikTok's conduct under its laws. Meta also selected California law as the law to govern all disputes with their customers in their respective terms of service. Defendants Meta and TikTok's

decision to reside in California and avail themselves of California's laws renders the application of California law to the claims herein constitutionally permissible.

183. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class, and California has a greater interest in applying its laws here given Defendants' locations and the location of the conduct at issue than any other interested state.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of the Plaintiff and the Class)
(Against all Defendants)

184. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

185. A Plaintiff asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff have a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

186. Defendants' surreptitious interception, storage, and use of Plaintiff's and Class members' interactions and communications with the Favor Platform, including PII, health information, and prescription requests, constitutes an intentional intrusion upon Plaintiff's and Class members' solitude or seclusion.

187. Plaintiff and Class members expected this information to remain private and confidential given the nature of the Favor Platform, which is primarily used to receive medical advice, treatment, and prescriptions.

188. This expectation is especially heightened given Favor's consistent representations that this data would remain confidential. Plaintiff and Class members did not expect third parties, and specifically Defendants, to secretly intercept this information and their communications.

189. Plaintiff and Class members did not consent to, authorize, or know about Defendants' intrusion at time it occurred. Plaintiff and Class members never agreed that Defendants could intercept, store, and use this data.

190. Defendants' intentional intrusion on Plaintiff's and Class members' solitude or seclusion would be highly offensive to a reasonable person. Plaintiff and Class members reasonably expected, based on Favor's repeated assurances, that their information would not be collected by Defendants.

191. The surreptitious taking and interception of sensitive data, including PII and medical information, from millions of individuals was highly offensive because it violated expectations of privacy that have been established by social norms. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

192. The offensiveness of this conduct is all the more apparent because Defendants' interception, storage, and use of this information was conducted inconspicuously in a manner that Plaintiff and Class members would be unable to detect and was contrary to the actual representations made by Favor.

193. Given the highly sensitive nature of the data that Defendants intercepted, such as private details about medications and health information, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

194. As a result of Defendants' actions, Plaintiff and Class members have suffered harm and injury, including, but not limited to, an invasion of their privacy rights.

195. Plaintiff and Class members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

196. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Defendants as a result of its intrusions upon Plaintiff's and Class members' privacy.

197. Plaintiff and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

198. Plaintiff also seeks such other relief as the Court may deem just and proper.

SECOND CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

199. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

200. Defendants received benefits from Plaintiff and Class members and unjustly retained those benefits at their expense.

201. Defendants received benefits from Plaintiff and Class members in the form of the Plaintiff's and Class members' highly valuable data, including health information and PII, that Defendants wrongfully intercepted from Plaintiff and Class members without authorization and proper compensation.

202. Defendants intercepted, stored, and used this data for their own gain, providing Defendants with economic, intangible, and other benefits, including highly valuable data for analytics, advertising, and improvement of their platforms, algorithms, and advertising services.

203. Had Plaintiff known of Defendants' misconduct, she would not have provided any of her data to Defendants or used the Favor Platform.

204. Defendants unjustly retained these benefits at the expense of Plaintiff and Class members because Defendants' conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

205. The benefits that Defendants derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles in California and every other state for Defendants to be permitted to retain any of the profit or other

benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

206. Defendants should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendants received, and such other relief as the Court may deem just and proper.

THIRD CLAIM FOR RELIEF
Violation of California Confidentiality of Medical Information Act ("CMIA")
Civil Code Section 56.36
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

207. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

208. California Civil Code Section 56.36(B)(3)(A) prohibits any person of entity other than a licensed health care professional from knowingly or willfully obtaining medical information for financial gain.

209. California Civil Code Section 56.36(B)(5) prohibits any person or entity who is not permitted to receive medical information under the CMIA from knowingly and willfully obtaining, disclosing, or using the medical information without written authorization.

210. Defendants are entities who are not licensed health care professionals, and Defendants are not permitted to receive medical information under the CMIA.

211. Defendants violated California Civil Code Section 56.36(B)(3)(A) and (B)(5) because they knowingly and willfully obtained medical information from the Favor Platform without authorization for their own financial gain.

212. As described herein, Defendants intentionally designed their software, i.e., the Meta Pixel and SDK, TikTok Pixel, and FullStory's session replay software, to intercept data from the websites and mobile applications in which they are incorporated.

213. Defendants knew this software was incorporated on websites and mobile applications that would consequently lead to the interception of medical information, including medical information input in the Favor Platform.

214. Defendants knowingly and willfully received this information without written authorization from Plaintiff and Class members and did so for their own financial gain. Namely, to profit through advertising and analytics services they offer, as well as to improve their algorithms, data points, and other technologies.

215. Pursuant to California Civil Code Section 56.36(B)(3)(A) and California Civil Code Section 56.36(B)(5), Defendants are liable for a civil penalty up to $250,000 per violation of these sections.

FOURTH CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code § 631
(On Behalf of Plaintiff and the Class and Subclass)
(Against all Defendants)

216. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

217. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA") finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

218. Cal. Penal Code § 631 imposes liability on any person who "by means of any machine, instrument, contrivance, or in any other manner" (1) "intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument," (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or

(4) "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

219. Defendants are persons for purposes of § 631.

220. Defendants Meta and TikTok maintain their principal places of business in California, where they designed, contrived, agreed, conspired, effectuated, and/or received the interception and use of the contents of Plaintiff's and Class members' communications. Additionally, Meta has adopted California substantive law to govern their relationship with users.

221. The Meta Pixel and SDK, the TikTok Pixel, and FullStory's session replay software, Plaintiff's and Class members' browsers and mobile applications, and Plaintiff's and Class members' computing and mobile devices are a "machine, instrument, contrivance, or . . . other manner."

222. At all relevant times, Meta, using its Meta Pixel and SDK, TikTok, using its TikTok Pixel, and FullStory, using its session replay software, intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiff and Class members and the Favor Platform without the consent of all parties to the communication.

223. Defendants, willfully and without the consent of Plaintiff and Class members, reads or attempt to reads, or learn the contents or meaning of Plaintiff's and Class members' communications to Favor while the communications are in transit or passing over any wire, line or cable, or were being received at any place within California when it intercepted Plaintiff's and Class members' communications and data with Favor, who is headquartered in California, in real time.

224. Defendants used or attempted to use the communications and information they received through their pixels, SDK, and session replay technology, including to supply analytics and advertising services.

225. The interception of Plaintiff's and Class members' communications was without authorization and consent from the Plaintiff and Class members. Accordingly, the interception was unlawful and tortious.

226. Plaintiff and the Class members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount

of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

227. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed, accessed, and stored by Defendants, has not been destroyed, and due to the continuing threat of such injury, Plaintiff and Class members have no adequate remedy at law, Plaintiff and Class members are entitled to injunctive relief.

FIFTH CLAIM FOR RELIEF
Violation of CIPA
Cal. Penal Code § 632
(On Behalf of Plaintiff and the Class and Subclass)
(Against all Defendants)

228. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

229. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

230. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

231. Plaintiff's and Class members' communications to Favor, including their sensitive medical information including information concerning medications they were taking or were prescribed, their medical histories, allergies, and answers to other health-related questions, were confidential communications for purposes of § 632, including because Plaintiff and Class members had an objectively reasonable expectation of privacy in this data.

232. Plaintiff and Class members expected their communications to Favor to be confined to Favor, in part because of Favor's consistent representations that these communications would remain confidential. Plaintiff and Class members did not expect third parties, and specifically Defendants, to secretly eavesdrop upon or record this information and their communications.

233. The Meta Pixel and SDK, the TikTok Pixel, and FullStory's session replay software are all electronic amplifying or recording devices for purposes of § 632.

234. By contemporaneously intercepting and recording Plaintiff's and Class members' confidential communications to Favor through the Meta Pixel and SDK, the TikTok Pixel, and session replay software, Defendants eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

235. At no time did Plaintiff or Class members consent to Defendants' conduct, nor could they reasonably expect that their communications to Favor would be overheard or recorded by Defendants.

236. Defendants utilized Plaintiff's and Class members' sensitive medical information for their own purposes, including advertising and analytics.

237. Plaintiff and Class members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

238. Plaintiff and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiff's and Class members' sensitive data has been collected, viewed, accessed, and stored by Defendants, has not been destroyed, and due to the continuing threat of such injury, Plaintiff and Class members have no adequate remedy at law, Plaintiff and Class members are entitled to injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Class and appointing Plaintiff as the Class' representative;

B. Finding that Defendants' conduct was unlawful, as alleged herein;

C. Awarding declaratory relief against Defendants;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper;

E. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

Dated: February 6, 2024

LYNCH CARPENTER, LLP

By: */s/ (Eddie) Jae K. Kim*

(Eddie) Jae K. Kim (CA Bar No. 236805)
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Tel.: (626) 550-1250
ekim@lcllp.com

LYNCH CARPENTER, LLP
Gary F. Lynch (admitted *pro hac vice*)
Jamisen A. Etzel (admitted *pro hac vice*)
Nicholas A. Colella (admitted *pro hac vice*)
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
Rachel Kesten (admitted *pro hac vice*)
Yuanchen Lu
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

Attorneys for Plaintiff and the Proposed Class